rapport certification MOOC ANSSI

Module 1 — Panorama de la cybersécurité

Le premier module introduit les fondamentaux de la cybersécurité.
Il permet de comprendre l'importance croissante de la sécurité numérique dans un monde où les systèmes informatiques sont omniprésents.

Ce qu'on apprend en détail :

- Les objectifs de la cybersécurité :
    - Confidentialité : seules les personnes autorisées peuvent accéder aux informations.
    - Intégrité : les données doivent rester exactes et non altérées.
    - Disponibilité : les systèmes et informations doivent rester accessibles lorsque nécessaire.
- Les différentes catégories de menaces :
    - Les malwares (virus, ransomwares, chevaux de Troie…).
    - Le phishing, qui vise à tromper l'utilisateur pour récupérer des données sensibles.
    - Les attaques DDoS, qui saturent un service pour le rendre indisponible.
    - L'espionnage et le sabotage informatique.
- Les motivations et profils des attaquants :
    - Cybercriminels cherchant un gain financier.
    - Hacktivistes défendant une cause idéologique.
    - États pratiquant la cyber-guerre ou l'espionnage stratégique.
    - Employés internes négligents ou malveillants.
- Les enjeux pour les particuliers, entreprises et institutions :
    - Protection des données personnelles.

    - Préservation de la réputation et de la confiance.
    - Sécurisation des infrastructures critiques (hôpitaux, transports, énergie…).
- Présentation de l'ANSSI :
    - Son rôle est de protéger l'État, accompagner les entreprises et sensibiliser la population.
    - Elle élabore des recommandations techniques, intervient en cas d'incident majeur et certifie des solutions de sécurité.

Conclusion du module :

Ce module pose les bases essentielles pour comprendre pourquoi la cybersécurité est un enjeu essentiel et comment les attaques sont organisées.

Module 2 — Sécurité de l'ordinateur et du mobile

Le deuxième module se concentre sur la protection des appareils utilisés au quotidien : ordinateurs, smartphones, tablettes.
Il aborde les risques techniques et les bonnes pratiques pour sécuriser ces dispositifs.

Ce qu'on apprend en détail :

- Configuration sécurisée du système :
    - Importance des mises à jour régulières du système d'exploitation et des applications.
    - Gestion des comptes utilisateurs (un compte administrateur, un compte standard).
    - Activation automatique des correctifs de sécurité.
- Logiciels et applications :
    - Installer uniquement des logiciels provenant de sources fiables.
    - Vérifier les permissions accordées aux applications mobiles.

    - Se méfier des logiciels piratés ou crackés, souvent porteurs de malwares.

- Solutions de protection :
    - Utilisation d'un antivirus reconnu.
    - Activation du pare-feu et configuration correcte.
    - Chiffrement du disque pour protéger les données en cas de vol.
- Gestion des périphériques externes :
    - Les clés USB représentent un vecteur d'infection très courant.
    - Importance d'utiliser des périphériques de confiance et de les analyser avant usage.
- Sauvegardes et récupération :
    - Différents types de sauvegardes (locale, cloud, sauvegarde système).
    - Mise en place d'une stratégie régulière pour éviter la perte de données.
    - Importance du stockage redondant pour la fiabilité.

Conclusion du module :

Ce module apprend à sécuriser efficacement les appareils qui constituent la première ligne de défense contre les cyberattaques.

Module 3 — Sécurité sur Internet

Dans ce module, on découvre les risques spécifiques liés à l'utilisation du réseau Internet et les méthodes pour naviguer en toute sécurité.

Ce qu'on apprend en détail :

- Fonctionnement de base d'Internet :
    - Le rôle du DNS pour traduire les noms de domaine.
    - Les adresses IP et la communication entre machines.

    - L’utilité du protocole HTTPS et des certificats SSL/TLS.
- Reconnaître un site fiable :
    - Vérification du cadenas HTTPS.
    - Contrôle du nom de domaine pour éviter les faux sites (typosquatting).
    - Importance des mises à jour du navigateur.
- Mail et phishing :
    - Reconnaître un mail frauduleux : fautes, adresse étrange, urgence exagérée.
    - Dangers des pièces jointes et des liens piégés.
    - Techniques utilisées par les pirates : usurpation, spear-phishing, etc.
- Risques des téléchargements :
    - Programmes pseudo-gratuits, cracks et extensions malveillantes.
    - Vérification de la source et de la réputation.
- Wi-Fi et réseaux publics :
    - Les risques d’interception des données sur des réseaux non sécurisés.
    - L’attaque du "man-in-the-middle".
    - Solutions : VPN, partage de connexion personnel, HTTPS systématique.
- Vie privée et traces numériques :
    - Gestion des cookies, trackers et profilage en ligne.
    - Paramétrage de la confidentialité dans les navigateurs.
    - Importance de maîtriser ses publications et données personnelles.

Conclusion du module :

L’utilisateur apprend à se protéger des dangers d’Internet en adoptant des réflexes de vigilance et en connaissant les outils disponibles.

Module 4 — Sécurité des données et des mots de passe

Ce module traite de la protection des données personnelles, professionnelles et stratégiques, ainsi que de la sécurisation des accès aux services numériques.

Ce qu'on apprend en détail :

- Nature et valeur des données :
    - Données personnelles : identité, santé, vie privée.
    - Données professionnelles : documents internes, secrets industriels.
    - Données sensibles : sécurité nationale, infrastructures.
- Risques liés aux données :
    - Perte ou vol de données.
    - Divulgation accidentelle.
    - Chantage et attaques par ransomware.
    - Mauvaise gestion du stockage.
- Chiffrement des données :
    - Chiffrement de fichiers, de disques ou de communications.
    - Principe de clé publique/clé privée.
    - Pourquoi le chiffrement protège même en cas de vol physique.
- Sauvegardes :
    - Règle 3–2–1 : 3 copies, 2 supports, 1 hors site.
    - Sauvegardes automatiques pour éviter l'oubli.
    - Tests de restauration.
- Sécurité des mots de passe :
    - Pourquoi un mot de passe doit être long, unique et complexe.

    - Méthodes pour créer un mot de passe solide (phrases secrètes…).
    - Risques des mots de passe réutilisés et faibles.
- Gestion des mots de passe :
    - Utilisation d’un gestionnaire de mots de passe.
    - Stockage sécurisé et synchronisation entre appareils.
- Authentification renforcée :
    - Double authentification (2FA) via SMS, application ou clé physique.
    - Limites de simple mot de passe.

Conclusion du module :

Ce dernier module enseigne comment protéger les données et sécuriser les comptes, ce qui est essentiel dans un contexte où presque toutes les informations sont numériques.